МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ШКОЛА № 141 ГОРОДСКОГО ОКРУГА САМАРА

РОССИЯ, 443084 г. Самара, ул. Каховская, 7
тел. (846) 992 50 00

«РАССМОТРЕНО»
на заседании методического
объединения учителей
_____
протокол № 1
от 30 августа 2023 г.
Председатель МО
_____/Вечканова М.

«УТВЕРЖДАЮ»
Директор МБОУ Школа № 141
_____/С.А. Габдрахманов/
Приказ № 393 от 31.08 2023 г.

«ПРОВЕРЕНО»
Заместитель директора по УВР
_____/Неизвестная Е.В.
30.08 2023 г.

РАБОЧАЯ ПРОГРАММА
факультативного курса

Информационная безопасность

для 5-6 классов

Пояснительная записка

(5-6 класс)

Рабочая программа факультативного курса «Информационная безопасность» (предметная область «Математика и информатика») составлена на основе:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

- Федеральным государственным образовательным стандартом основного общего образования, утвержденным приказом Минпросвещения от 31.05.2021 № 287 (далее – ФГОС ООО);

- Приказом Министерства просвещения Российской Федерации от 16 ноября 2022 г. №992 «Об утверждении федеральной образовательной программы основного общего образования»;

- Постановлением Главного государственного врача РФ от 28.01.2021г.№2 «Об утверждении СанПиН 1.2.3685-21» «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»;

- Основной образовательной программы основного общего образования МБОУ Школы №141 г.о. Самара;

- Положения о рабочей программе МБОУ Школы №141 г.о. Самара.

Факультативный курс «Информационная безопасность» в основной школе изучается в 5-6 классе. Общее количество часов составляет 68 часа. В 5 классе – 34 часа и в 6 классе – 34 часа.. Количество часов - 1 час в неделю.

ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ФАКУЛЬТАТИВОГО КУРСА «ИНФОРМЦИОННАЯ БЕЗОПАСНОСТЬ»

Изучение факультативного курса «Информационная безопасность» позволяет гармонично сочетать обучение современным информационным технологиям и формирование информационной культуры, высоких нравственных качеств, способствует выработке иммунитета к совершению неэтичных, противоправных действий в сфере информационных технологий. Факультатив ориентирован на подготовку подрастающего поколения к жизни и деятельности в совершенно новых условиях информационного общества, в котором вопросы обеспечения информационной безопасности личных, общественных и государственных информационных ресурсов особенно актуальны. Развитие глобального процесса информатизации общества, захватывающего все развитые и многие развивающиеся страны мира, приводит к формированию новой информационной среды, информационного уклада и профессиональной деятельности. Однако при этом пропорционально возрастает уязвимость личных, общественных и государственных информационных ресурсов со стороны негативного воздействия средств информационно-коммуникационных технологий. Таким образом, мировое сообщество стоит перед глобальной социотехнической проблемой – проблемой обеспечения информационной безопасности. Решение проблемы безопасности вообще и информационной безопасности в частности невозможно без достаточного количества как высококвалифицированных профессионалов, так и квалифицированных пользователей, компетентных в сфере защиты информации. Данный факультатив преследует следующие **цели:**

-Овладение учащимися умениями: профилактики, защиты программного обеспечения; обнаружения и удаления компьютерных вирусов; защиты информации в автоматизированных системах обработки данных, в глобальной сети Интернет.

-Приобретение учащимися опыта по предупреждению и нейтрализации негативного воздействия информационных угроз на людей и программно-технические комплексы; опыта информационной деятельности в сферах обеспечения защиты информации, актуальных на рынке труда.

-Приобретения учащимися опыта создания, редактирования, оформления, сохранения, передачи информационных объектов различного типа с помощью современных программных средств;

коллективной реализации информационных проектов, преодоления трудностей в процессе проектирования, разработки и реализации учебных проектов.

Перед данным элективным курсом ставятся следующие задачи: образовательные:

-освоение учащимися знаний, относящихся к основам обеспечения информационной безопасности, и их систематизация;

-изучение учащимися мер законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в системах связи;

развивающие:

-повышение интереса учащихся к изучению информатики;

-приобретение учащимися навыков самостоятельной работы с учебной, научно-популярной литературой и материалами сети Интернет;

-развитие у учащихся способностей к исследовательской деятельности;

воспитательные:

-воспитание у учащихся культуры в области применения ИКТ в различных сферах современной жизни;

-воспитание у учащихся чувства ответственности за результаты своего труда, используемые другими людьми;

-воспитание у учащихся умения планировать, работать в коллективе;

-воспитание у учащихся нравственных качеств, негативного отношения к нарушителям информационной безопасности;

-воспитание у учащихся установки на позитивную социальную деятельность в информационном обществе, недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Предметные результаты:

основные понятия и определения из области обеспечения информационной безопасности; методы и средства борьбы с угрозами информационной безопасности; классификацию вредоносных программ и их влияние на целостность информации; порядок заражения файлов; методы проведения профилактики, защиты и восстановления пораженных вредоносными программами объектов; нормативные руководящие документы, касающиеся защиты информации, существующие стандарты информационной безопасности; принципы выбора пароля, аппаратные и программные средства для аутентификации по паролю; основные понятия криптографических методов защиты информации, механизмы цифровой электронной подписи; существующие программные продукты, предназначенные для защиты электронного обмена данными в Интернете, способы отделения интрасети от глобальных сетей; нормы информационной этики и права.

Метапредметные результаты:

Метапредметные результаты освоения основной образовательной программы **представлены тремя группами универсальных учебных действий (УУД)**:

Регулятивные универсальные учебные действия

- умение самостоятельно определять цели, задавать параметры и критерии, по которым можно определить, что цель достигнута;
- умение ставить и формулировать собственные задачи в образовательной деятельности и жизненных ситуациях;
- умение оценивать ресурсы, в том числе время и другие нематериальные ресурсы, необходимые для достижения поставленной цели;
- умение выбирать путь достижения цели, планировать решение поставленных задач, оптимизируя материальные и нематериальные затраты;
- умение сопоставлять полученный результат деятельности с поставленной заранее целью.
- умение оценивать возможные последствия достижения поставленной цели в деятельности, собственной жизни и жизни окружающих людей, основываясь на соображениях этики и морали;
- умение организовывать эффективный поиск ресурсов, необходимых для достижения поставленной цели;

Познавательные универсальные учебные действия

- умение искать и находить обобщенные способы решения задач, в том числе, осуществлять развернутый информационный поиск и ставить на его основе новые (учебные и познавательные) задачи;
- умение использовать различные модельно-схематические средства для представления существенных связей и отношений, а также противоречий, выявленных в информационных источниках;
- умение находить и приводить критические аргументы в отношении действий и суждений другого; спокойно и разумно относиться к критическим замечаниям в отношении собственного суждения, рассматривать их как ресурс собственного развития;
- умение выстраивать индивидуальную образовательную траекторию, учитывая ограничения со стороны других участников и ресурсные ограничения;
- умение критически оценивать и интерпретировать информацию с разных позиций, распознавать и фиксировать противоречия в информационных источниках;
- умение выходить за рамки учебного предмета и осуществлять целенаправленный поиск возможностей для широкого переноса средств и способов действия;
- умение менять и удерживать разные позиции в познавательной деятельности.

Коммуникативные универсальные учебные действия

- умение осуществлять деловую коммуникацию, как со сверстниками, так и со взрослыми (как внутри образовательной организации, так и за ее пределами), подбирать партнеров для деловой коммуникации исходя из соображений результативности взаимодействия, а не личных симпатий;
- умение координировать и выполнять работу в условиях реального, виртуального и комбинированного взаимодействия;
- умение развернуто, логично и точно излагать свою точку зрения с использованием адекватных (устных и письменных) языковых средств;
- умение при осуществлении групповой работы быть как руководителем, так и членом команды в разных ролях (генератор идей, критик, исполнитель, выступающий, эксперт и т.д.);

умение распознавать конфликтогенные ситуации и предотвращать конфликты до их активной фазы, выстраивать деловую и образовательную коммуникацию, избегая личностных оценочных суждений.

Личностными результатами изучения курса следует считать воспитание мотивации к труду, стремления строить свое будущее на основе целеполагания и планирования, ответственности за благополучие своей семьи и государства.

Учет воспитательного потенциала уроков

Целью школьного информационного образования является формирование у обучающегося ответственного и избирательного отношения к информации с учётом правовых и этических аспектов её распространения, стремления к продолжению образования в области информационных технологий и созидательной деятельности с применением средств информационных технологий. Особое значение приобретает представление о социальных нормах и правилах межличностных отношений в коллективе, в том числе в социальных сообществах; соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде; готовность к разнообразной совместной деятельности при выполнении учебных, познавательных задач, создании учебных проектов; стремление к взаимопониманию и взаимопомощи в процессе этой учебной деятельности; готовность оценивать своё поведение и поступки своих товарищей с позиции нравственных и правовых норм с учётом осознания последствий поступков.

Рабочая программа факультативного курса «Информационная безопасность» входит в предметную область «Математика и информатика». Учитывая образовательные запросы обучающихся и их родителей факультативный курс «Информационная безопасность» взят из части, формируемой участниками образовательных отношений.

Изучение факультативного курса «Информационная безопасность» предполагает активную социокультурную деятельность обучающихся, участие в исследовательских и творческих проектах. Способы проверки ожидаемых результатов, предусмотренных программой, это устные опросы, письменные опросы, беседа, наблюдения, самостоятельные работы, участие в конкурсах различного уровня.

Воспитательный потенциал факультативного курса «Информационная безопасность» реализуется через:

- привлечения внимания учащихся к ценностному аспекту изучаемых на уроках явлений, организация их работы с получаемой на уроке социально значимой информации – инициирование ее обсуждения, высказывания учащимися своего мнения по ее поводу, выработки своего к ней отношения.
- демонстрацию обучающимся видеосюжетов, кинофильмов, устройств, технических установок для разнообразия подачи материала и поднятия интереса обучающихся к изучаемому предмету, что подталкивает их к получению дополнительной информации через самообучение.
- применение на уроке интерактивных форм работы с обучающимися: интеллектуальных игр, стимулирующих познавательную мотивацию обучающихся;
- инициирование и поддержку исследовательской деятельности обучающихся в рамках реализации ими индивидуальных и групповых исследовательских проектов, что даст обучающимся возможность приобрести навык самостоятельного решения теоретической проблемы, навык генерирования и оформления собственных идей, навык уважительного отношения к чужим идеям, оформленным в работах других исследователей, навык публичного выступления перед аудиторией, аргументирования и отстаивания своей точки зрения.

СОДЕРЖАНИЕ КУРСА

5 класс

1. ***Общие проблемы информационной безопасности.***

Информация и информационные технологии. Актуальность проблемы обеспечения безопасности информационных технологий. Основные термины и определения. Субъекты информационных отношений, их интересы и безопасность. Конфиденциальность, целостность, доступность. Пути нанесения ущерба. Цели и объекты защиты.

2. ***Угрозы информационной безопасности.***

Понятие угрозы. Виды проникновения или «нарушителей». Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам. Каналы утечки информации и их характеристика.

3. ***Вредоносные программы. Методы профилактики и защиты.***

Общие сведения о вредоносных программах. Классификация по среде обитания, поражаемой операционной системе, особенностям алгоритма работы. Принципы функционирования, жизненный цикл и среда обитания компьютерных вирусов. Симптомы заражения и вызываемые вирусами эффекты. Полиморфные и стелс-вирусы. Вирусы-макросы для Microsoft Word и Microsoft Excel. Вирусы-черви. Профилактика заражения. Программные антивирусные средства. Определения и общие принципы функционирования фагов, детекторов, ревизоров, вакцин, сторожей. Структура антивирусной программы. Виды антивирусных программ.

4. ***Правовые основы обеспечения информационной безопасности.***

Законодательство в информационной сфере. Виды защищаемой информации. Государственная тайна как особый вид защищаемой информации; система защиты государственной тайны; правовой режим защиты государственной тайны. Конфиденциальная информация. Лицензионная и сертификационная деятельность в области защиты информации. Основные законы и другие нормативно-правовые документы, регламентирующие деятельность организации в области защиты информации. Защита информации ограниченного доступа. Ответственность за нарушение законодательства в информационной сфере. Информация как объект преступных посягательств. Информация как средство совершения преступлений. Отечественные и зарубежные стандарты в области информационной безопасности.

5. ***Современные методы защиты информации в автоматизированных системах обработки данных.***

Обзор современных методов защиты информации. Основные сервисы безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит. Криптографическое преобразование информации. История

криптографии; простейшие шифры и их свойства. Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. Электронная цифровая подпись. Контроль целостности; экранирование; анализ защищѐнности; обеспечение отказоустойчивости; обеспечение безопасного восстановления.

6. ***Технические и организационные методы защиты информации.***

Технические средства охраны объектов (физическая защита доступа, противопожарные меры). Защита от утечки информации (перехвата данных, электростатических и электромагнитных излучений и др.). Технические средства противодействия несанкционированному съѐму информации по возможным каналам ее утечки. Организационные меры защиты. Определение круга лиц, ответственных заинформационную безопасность, обеспечение надѐжной и экономичной защиты. Требования к обслуживающему персоналу.

7. ***Технические и организационные методы защиты информации.***

Технические средства охраны объектов (физическая защита доступа, противопожарные меры). Защита от утечки информации (перехвата данных, электростатических и электромагнитных излучений и др.). Технические средства противодействия несанкционированному съѐму информации по возможным каналам еѐ утечки. Организационные меры защиты. Определение круга лиц, ответственных заинформационную безопасность, обеспечение надѐжной и экономичной защиты. Требования к обслуживающему персоналу.

8. ***Защита информации в компьютерных сетях.***

Примеры взломов сетей и веб-сайтов. Причины уязвимости сети Интернет. Цели, функции и задачи защиты информации в компьютерных сетях. Безопасность в сети Интернет. Методы атак, используемые злоумышлиниками для получения или уничтожения интересующей информации через Интернет. Способы отделения интрасети от глобальных сетей. Фильтрующий маршрутизатор, программный фильтр и т.д.

9. ***Проблемы информационно–психологической безопасности личности.***

Определение понятия информационно-психологической безопасности.Основные виды информационно-психологических воздействий. Виртуальная реальность и еѐ воздействие на нравственное, духовное, эмоциональное и физическое здоровье школьников. Игромания, компьютерные манипуляции, фишинг, киберугрозы и пропаганда других опасных явлений в Интернете. Способы Защиты от нежелательной информации в Интернете. Нравственно-этические проблемы информационного общества.

6 класс

1. Общие сведения о безопасности ПК и Интернета (5 часов).

Как устроены компьютер и интернет. Как работают мобильные устройства. Угрозы для мобильных устройств. Защита персональных данных, почему она нужна. Категории персональных данных. Биометрические персональные данные. Безопасный профиль в социальных сетях. Составление сети контактов. Защита киберпространства как комплекс мероприятий, направленных на обеспечение информационной безопасности. Аспекты кибербезопасности. Компьютерная и информационная безопасность, обнаружение проблем сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Основные угрозы безопасности информации: утечки, потеря целостности, нарушение работоспособности системы, незаконное тиражирование (воспроизведение). Безопасный серфинг. Безопасные ресурсы для поиска.

Практическая работа. Составить информационный буклет «Моя безопасная сеть» или сделать групповую газету «Безопасность в Интернет».

2. Техника безопасности и экология (5 часов).

Правила поведения в компьютерном классе. Техника безопасности при работе с компьютером. Компьютер и мобильные устройства в чрезвычайных ситуациях. Компьютер и зрение. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM). Комплекс упражнений при работе за компьютером. Гигиена при работе с ПК

Практическая работа. Создание буклета «Техника безопасности при работе с компьютером».

3. Проблемы Интернет-зависимости (5 часов).

ЗОЖ и компьютер. Деструктивная информация в Интернете - как ее избежать. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютерная зависимость (аддикция). Критерии зависимости с точки зрения психологов (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Как развивается зависимость. Типы интернет - зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения, сексуальные зависимости).

Практическая работа. «Создание мультимедийной презентации «ПК и ЗОЖ. Организация рабочего места».

4. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы. (6 часов).

Вирусы человека и компьютера, цели компьютерных вирусов. Типы вирусов. Отличия вирусов и закладок. Как распространяются вирусы. Что такое антивирусная защита. Как лечить компьютер. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов. Защита мобильных устройств. Безопасность при скачивании файлов. Защита программ и данных от несанкционированного копирования. Организационные, юридические, программные и программно-аппаратные меры защиты. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Методы защиты фото и видеоматериалов от копирования в сети. Проверка подлинности (аутентификация) в Интернете. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.

Практическая работа «Установка антивирусной программы»;

Практическая работа. Создание презентации на тему: «Разновидности вирусов Черви, трояны, скрипты», «Шпионские программы», «Шифровальщики». «Троян-вымогатель в социальной сети “ВКонтакте” или наказание для особо любопытных».

5. Мошеннические действия в Интернете. Киберпреступления. (5 часов).

Виды интернет - мошенничества (письма, реклама, охота за личными данными и т.п.). Фишинг (фарминг). Мошеннические действия в сети. Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в

Интернете. Пирамиды. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн - казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею. Технологии манипулирования в Интернете. Техника безопасности при интернет - общении.

Практическая работа. Доклад на тему: «Правила поведения в сети с мошенниками и злоумышленниками», или «Как не стать жертвой сетевых шуток и розыгрышей».

6. Сетевой этикет. Психология и сеть. (5 часов).

Что такое этикет. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах. Как появился этикет, что это такое. Сетевой этикет. Общие правила сетевого этикета. Этика дискуссий. Взаимное уважение при интернет-общении. Этикет и безопасность. Эмоции в сети, их выражение. Примеры этических нарушений. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибер-моббинг, троллинг, буллицид. Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений).

Практическая работа. «Выпуск видеоролика на тему «Как не испортить себе настроение при общении в Сети и не опуститься до уровня «веб-агрессора».

7. Государственная политика в области кибербезопасности. (3 часов).
Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера. Как расследуются преступления в сети. Ответственность за интернет- мошенничество. Правовые акты в области информационных технологий и защиты киберпространства. Доктрина информационной безопасности.

Практическая работа «Буклет. Правовые основы для защиты от спама».

Практическая работа. Создание презентации «Как уберечь свою персональную информацию в Интернете, если вы общаетесь в социальных сетях».

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Разделы, модули, темы	Количество часов/из них контрольных, лабораторных, практических работ			
		всего	по классам		к/р / пр.
			5 кл.	6 кл.	
1	Общие проблемы информационной безопасности	2	0/1		
2	Угрозы информационной безопасности.	2	0/1		
3	Вредоносные программы. Методы профилактики и защиты	4	1/1		
4	Правовые основы обеспечения информационной безопасности	4	0/1		
5	Современные методы защиты информации в автоматизированных системах обработки данных	8	1/1		
6	Технические и организационные методы защиты информации	2	0/1		
7	Защита информации в компьютерных сетях	7	0/1		
8	Проблемы информационно–психологической безопасности личности	5	1/1		
9	Общие сведения о безопасности ПК и Интернета	5		0/1	
10	Техника безопасности и экология	5		1/1	
11	Проблемы Интернет-зависимости	5		0/1	
12	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	6		1/2	
13	Мошеннические действия в Интернете. Киберпреступления	5		0/1	
14	Сетевой этикет. Психология и сеть	5		1/1	
15	Государственная политика в области кибербезопасности	3		0/1	
	Общее количество часов	34	3/8	3/8	6/16

Планирование 5 класс

№ п/п	Раздел /тема	Количество часов, отводимых на освоение темы	Электронные учебно-методические материалы
1	Общие проблемы информационной безопасности	2	https://lbz.ru/metodist/authors/ib/5-6.php
	Основные понятия информационной безопасности.	1	
	Актуальность проблемы обеспечения безопасности ИТ. Практическая работа 1	1	
2	Угрозы информационной безопасности	2	https://lbz.ru/metodist/authors/ib/5-6.php
	Понятие угрозы информационной безопасности	1	
	Классификация видов угроз информационной. Практическая работа 2	1	
3	Вредоносные программы. Методы профилактики и защиты	4	https://lbz.ru/metodist/authors/ib/5-6.php
	Общие сведения о вредоносных программах. Компьютерные вирусы	1	
	Профилактика заражения	1	
	Методы защиты компьютеров от вредоносных программ. Практическая работа 3	1	
	Программные антивирусные средства. Антивирусные программы. Контрольная работа 1 по разделу «Вредоносные программы»	1	
4	Правовые основы обеспечения информационной безопасности	4	https://lbz.ru/metodist/authors/ib/5-6.php
	Законодательство в области защиты информации. Преступление и наказание в сфере информационных	1	
	Отечественные и зарубежные стандарты в области информационных технологий	1	
	Защита информации ограниченного доступа.	1	
	Государственная тайна как особый вид защищаемой информации. Практическая работа 4	1	
5	Современные методы защиты информации в автоматизированных системах обработки данных	8	https://lbz.ru/metodist/authors/ib/5-6.php
	Основные сервисы безопасности. Правила создания и замены паролей. Идентификация и аутентификация	1	
	Управление доступом. Протоколирование и аудит.	2	
	Криптография. Криптографическая защита.	1	
	Электронная цифровая подпись.	1	

	Криптографические методы защиты информации	1	
	Контроль целостности; экранирование; анализ защищенности. Практическая работа 5	1	
	Обеспечение отказоустойчивости и безопасного восстановления. Контрольная работа 2 по разделу «Современные методы защиты информации в автоматизированных системах обработки данных»	1	
6	Технические и организационные методы защиты информации	2	https://lbz.ru/metodist/authors/ib/5-6.php
	Технические средства защиты информации	1	
	Организационные меры защиты. Практическая работа 6	1	
7	Защита информации в компьютерных сетях	7	https://lbz.ru/metodist/authors/ib/5-6.php
	Защита информации в компьютерных сетях	1	
	Безопасность в сети Интернет.	1	
	Защита электронного обмена данных в интернете.	2	
	Способы отделения интрасети от глобальных сетей.	1	
	Фильтрующий маршрутизатр, программный фильтр, системы типа FireWall	1	
	Фильтрующий маршрутизатор, программный фильтр, системы типа FireWall. Практическая работа 7	1	
8	Проблемы информационно–психологической безопасности личности	5	https://lbz.ru/metodist/authors/ib/5-6.php
	Информационно-психологическая безопасность личности в информационном обществе	1	
	Виртуальная реальность и ее воздействие на нравственное, духовное, эмоциональное и физическое здоровье школьников	1	
	Нравственно–этические проблемы информационного общества	1	
	Способы защиты от нежелательной информации в Интернете. Практическая работа 8	1	
	Контрольная работа 3 по разделу «Проблемы информационно психологической безопасности личности»	1	

Планирование 6 класс

№ п/п	Раздел /тема	Количество часов, отводимых на освоение темы	Электронные учебно-методические материалы
1	Общие сведения о безопасности ПК и Интернета	5	https://lbz.ru/metodist/authors/ib/5-6.php
	Техника безопасности и организация рабочего места. Как устроен компьютер и Интернет.	1	
	Защита персональных данных, почему она нужна.	1	
	Защита киберпространства.	1	
	Основные угрозы безопасности информации.	1	
	Практическая работа №1. Сделать газету «Безопасность в Интернет»	1	
2	Техника безопасности и экология	5	https://lbz.ru/metodist/authors/ib/5-6.php
	Компьютер и мобильные устройства в чрезвычайных ситуациях	1	
	Воздействие радиоволн на здоровье и окружающую среду	1	
	Техника безопасности при работе с компьютером	1	
	Компьютерная техника и экология. Контрольная работа 1 по разделу «Техника безопасности и экология»	1	
	Практическая работа №2. Создание буклета «Техника безопасности при работе с компьютером»	1	
3	Проблемы Интернет-зависимости	5	https://itprojects.narfu.ru/cybersecurity/school-materials.php
	Деструктивная информация в Интернете-как ее избежать	1	
	Психологическое воздействие информации на человека.	1	
	Управление личностью через сеть.	1	
	Интернет и компьютерная зависимость.	1	
	Практическая работа №3. Создание презентации «ПК и ЗОЖ. Организация рабочего места»	1	
4	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	6	https://lbz.ru/metodist/authors/ib/5-6.php
	Компьютерные вирусы	1	
	Инструктаж по технике безопасности на рабочем месте.	1	
	Организационные, юридические меры защиты.	1	
	Меры защиты ПК, аккаунтов, мобильных устройств. Контрольная работа 2 по разделу «Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы»	1	
	Практическая работа №4. «Установка	1	

	антивирусной программы»		
	Практическая работа №5. Создание презентации на тему «Вирус»	1	
5	Мошеннические действия в Интернете. Киберпреступления	5	https://itprojects.narfu.ru/cybersecurity/school-materials.php
	Виды интернет- мошенничества.	1	
	Мошенничество при распространении «бесплатного» ПО	1	
	Опасности мобильной связи	1	
	Технология манипулирования в интернете	1	
	Практическая работа №6. Доклад «Правила поведения в сети с мошенниками и злоумышленниками»	1	
6	Сетевой этикет. Психология и сеть	5	https://lbz.ru/metodist/authors/ib/5-6.php
	Что такое этикет. Этика и безопасность	1	
	Безопасная работа в сети	1	
	Психологическая обстановка в Интернете	1	
	Психологическая обстановка в Интернете. Контрольная работа 3 по разделу «Сетевой этикет. Психология и сеть»	1	
	Практическая работа №7. Видеоролик на тему «Как не испортить себе настроение в Сети и не опуститься до уровня «веб-агрессора»	1	
7	Государственная политика в области кибербезопасности	3	https://lbz.ru/metodist/authors/ib/5-6.php
	Собственность в Интернете	1	
	Защита прав потребителей при использовании услуг Интернета	1	
	Доктрина информационной безопасности. Практическая работа №8	1	